REMARKS

Applicant gratefully acknowledges the courtesy of the Examiner in granting an interview to Applicant's representatives Sanford T. Colb, registration number 26,856, and David Zviel, registration number 41,392, on 28 February 2005. Supervisory Examiner Syed Zia was also present at the interview.

In the interview, independent claim 78 was discussed in detail to elaborate the differences between the present application and the references cited by the examiner. In preferred embodiments of the present invention as claimed, for example, in claim 78, the player authenticates itself to the medium, as opposed to the medium authenticating itself to the player, as in the references cited by the examiner. The fact that in US Patent 5,881,152 to Moos, for example, the medium includes only a memory chip, which is incapable of authenticating the player, was also discussed. It was agreed that upon filing a formal response, further searching will be conducted.

Applicant has carefully studied the outstanding Official Action. The present amendment is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

Claims 78, 80 - 82, and 84 - 86 stand rejected in the present application. Claims 96 - 102 have been added.

Claims 78, 80, 81 and 84 stand rejected under 35 USC 103(a) as being unpatentable over US Patent 5,881,152 to Moos.

Moos describes a process and device for combining non-intelligent generic information storage devices with intelligent storage devices and linking their information. The process compresses the stored data from a generic storage device and counts a signature count of the stored data. An ID is then provided to the stored data from a permanently assigned intelligent programmable memory chip. At least part of the compressed data is encrypted using an asymmetric key and transferred to a memory area of the permanently assigned intelligent

programmable memory chip. Moos nowhere describes or suggests providing any chip other than a memory chip in the information storage device.

Moos (col. 3, lines 6 -14) states: "An authorized target system can uniquely identify a data storage device thus secured. For this purpose, a challenge and response exchange is carried out between the software and the chip and thus the validity of the data storage device is established. Subsequently the data is read in the conventional manner and compressed with the same algorithm used for writing. The cryptogram obtained after writing to the data storage device is read from the memory of the chip and decoded using the public part of the asymmetric key." Namely, the medium authenticates itself to the player.

In the present invention, by contrast, as claimed in claim 78, "said disk security chip, after assuring that said DVD player is authentic, sends said DVD player said disk key" (emphasis added). That is, the player is authenticated to the medium.

Applicant wishes to respectfully call the Examiner's attention to the following additional arguments:

After challenge response, that is, after "validity of data storage device is established", Moos (see col. 3, lines 1 -14) reads data in a "conventional manner and compressed with the same algorithm used for writing." In the present invention, as claimed in claim 78, by contrast to Moos, the disk key is sent after establishing the validity of the DVD player.

Additionally, Moos does not require first showing authenticity before sending the key. In the present invention, as claimed in claim 78, by contrast to Moos, a showing of authenticity is first required.

Claim 78 is therefore deemed allowable.

Regarding claim 84, Applicant respectfully points out that Moos does not indicate that the disk key is encrypted with the player key before the sending. In the present invention, as claimed in claim 84, in contrast to Moos, said DVD player sends said disk key encrypted with said player key.

Furthermore, Moos uses symmetric key challenge response to establish identification of the data storage device. In the present invention, as claimed in claim 84, in contrast to Moos, it is ensured that "said DVD player is

authentic..." Authentication and identification are NOT the same. Identification asks the question: "who are you?" Authentication demands: "prove that you are who you say that you are". (see Bruce Schneier, Beyond Fear, pp. 182 - 183).

Claims 80, 81 and 84 depend from claim 78 and recite additional patentable subject matter.

Claims 80, 81 and 84 are therefore deemed allowable in light of the discussion of the allowability of claim 78, and, with respect to claim 84, in light of the above argument.

Claim 82 stands rejected in light of Moos as modified by Menezes (Handbook of Applied Cryptography).

Menezes et al., on pages 406 - 410 describe zero knowledge identification protocols.

Claim 82 depends from claim 78 and recites additional patentable subject matter.

Claim 82 is therefore deemed allowable with reference to the above discussion of the allowability of claim 78.

Claims 85 and 86 stand rejected in light of Moos in view of Litman (5,988,500).

Litman describes a system and method of inserting magnetic elements into items in order to provide readable magnetic patterns which provide reproducible or unique signals to identify or authenticate items.

Litman is from a field of art unrelated to the present invention and to Moos. Applicant respectfully therefore points out that, in order to properly reject claims 85 and 86, the Examiner needs to make an argument stronger than merely asserting that it would have been obvious to one skilled in the art to combine Litman with Moos.

In any event, claims 85 and 86 depend, either directly or indirectly from claim 78 and recite additional patentable subject matter.

Claims 85 and 86 are therefore deemed allowable with reference to the above discussion of the allowability of claim 78.

New claim 96 has been added. New claim 96 corresponds to claim 78, without the limitation of "providing said disk security chip with a disk key not

known to a disk manufacturer", which limitation is deemed unnecessary in order to distinguish the present invention over the art of record.

New claim 96 is supported, inter-alia, by pages 6, 7, 8, and 12 - 14 of the disclosure, and by Figs. 4 and 5.

New claims 97 - 99 correspond to claims 80 - 82.

New claims 100 - 102 correspond to claims 84 - 86.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,

JULIAN COHEN
c/o LADAS & PARRY LLP
26 WEST 61st STREET
NEW YORK, N. Y. 10023
Reg. No. 20302 (212) 708-1887